Proceedings of the 34th Hawaii International Conference on System Sciences - 2001

Development of Personal Authentication System Using Fingerprint with Digital Signature Technologies

Yoshiaki Isobe*, Yoichi Seto*, and Masanori Kataoka**
*: *Systems Development Laboratory, Hitachi, Ltd.*
{ isobe, seto }@sdl.hitachi.co.jp
**: *Hitachi netBusiness, Ltd.*
m-kataoka@hi-nb.com

Abstract

Authentication based on biometrics is being applied to control physical access to high-security facilities. Recently, with the recent rapid growth of information system technologies, applications for accessing databases or business workflow systems have begun to use biometrics. These applications need to implement measures to counter threats to security. In the case of authentication through an open network, such as non-face-to-face trading, the integrity of data is important. We have to guarantee the integrity of the registered biometric data. This paper presents a biometrics-based personal authentication system in which a smart card, a Public Key Infrastructure (PKI) such as an X.509 certificate, and fingerprint verification technologies are combined. We have developed a prototype system in which the system is applied to a business workflow. The proposed system can also be applied to some public key platforms such as the 'electronic signature act', because our system has been developed on equivalent platforms.

1. Introduction

Electronic commerce based on an open network is gradually being established as part of daily life. In the non-face-to-face transactions of electronic commerce, personal authentication technology for verifying the identity of the persons involved is very important. Biometric techniques, which use physical data, are receiving attention as a personal authentication method that is more convenient than conventional methods such as a password or ID cards.

Biometric personal authentication uses data taken from measurements of a person's body, such as fingerprints, faces, irises, retinal patterns, palm prints, voice prints, hand-written signatures, and so on, to identify individuals by means of image processing or signal processing[1) 2)]. Such data is unique to the individual and remains so throughout one's life. This technology has been applied for controlling access to high-security facilities, but it is now being investigated for application to information systems such as electronic commerce[3)]. However, the security function requirements differ greatly for personal authentication in these kinds of applications and personal authentication in facility access control, so it is important to study these security function requirements, which include the overall security (threat-countering capability) of the network system.

In investigating these requirements in an open network, because we believe that the cooperation between smart card technology and public-key encryption technology is important[4) 5)], we have been developing smart card owner authentication technology[6) 7)]. However, there remains the problem of guaranteeing the validity of the biometric data that is stored in the terminal or smart card against counterfeiters or other kinds of corruption.

This paper addresses the problem of securing the validity of the biometric data that is stored in smart cards and describes our study of a personal authentication system that employs fingerprint data that is protected by an X.509 certificate. In Section 2, an overview of biometrics-based personal authentication is presented. In Section 3, this paper describes the results of our investigation of personal authentication system technologies in detail. The development of a prototype system is described in Section 4.

2. Personal authentication technology based on biometrics

2.1. The use of biometrics in personal

0-7695-0981-9/01 $10.00 (c) 2001 IEEE

authentication technology

In biometrics-based personal authentication, biometric data that is to be used for reference in comparison (referred to as template data) is registered in advance in the same way as when passwords are used. In the authentication processing, another biometric data that was input from a sensor is compared with the pre-registered template data and a degree of similarity is calculated. This degree of similarity serves as the basis for deciding whether or not this person is the authorized person.

Personal authentication technology that uses biometrics checks for the authorized person by means of image (or signal) processing techniques. For this reason, personal authentication may not be possible for characteristic information that is outside the assumptions of the sensors or algorithms. (This is evaluated on the basis of a standard that is referred to as the correspondence rate[3]). Also, differences in recognition conditions such as the environmental temperature and the physical condition of the person may result in wrongly rejecting the authorized person or wrongly accepting a non-authorized person [8].

It is necessary to understand the recognition accuracy and incorporate it into the application.

2.2. Comparison with conventional applications

Biometric personal authentication technology has been applied to the control of physical access, such as entry to high-security facilities.

Physical access control involves using personal authentication equipment only to control the opening and closing of doors, etc. The maintenance of security requirements such as data secrecy is easy because there is only concern for security within the equipment (Fig. 1(a)).

In recent years, the development of information systems and the lower cost of biometric personal authentication technology have spurred research on the following kinds of electronic applications.

(a) Access control systems for databases, etc.
(b) Electronic decision/authorization systems

For the simple application of personal authentication equipment that is used to control physical access to such systematic applications, it is no more than a matter of securing the data and functions inside the computer to which the personal authentication equipment is connected. The problem is that the validity of the following kinds of data and processing cannot be confirmed in the case of authentication over a network, as shown in Fig. 1(b).

- The templates registered in the personal authentication equipment
- The template for the user's ID
- The comparison function of the personal authentication equipment
- The biometric data that has been input to the comparison equipment

Because of this, in order for data and functions to be provided over a network, systematic personal authentication measures are required to guarantee security.

ECOM (The Electronic Commerce Promotion Council of Japan) [5] proposed the following six kinds of evaluation standards (Criteria), which include resistance to attack. These standards have been proposed as requirements for personal authentication by means of biometrics.

(1) Social acceptability
(2) User acceptability
(3) Threat countermeasure
(4) Accuracy of authentication
(5) Ease of use
(6) Maintenance and Administration

In the research presented here, we investigated personal authentication system technology on the basis of these evaluation standards.

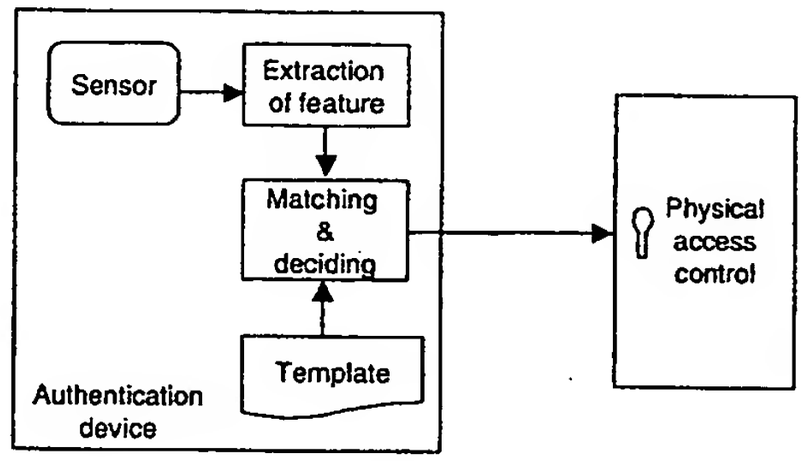


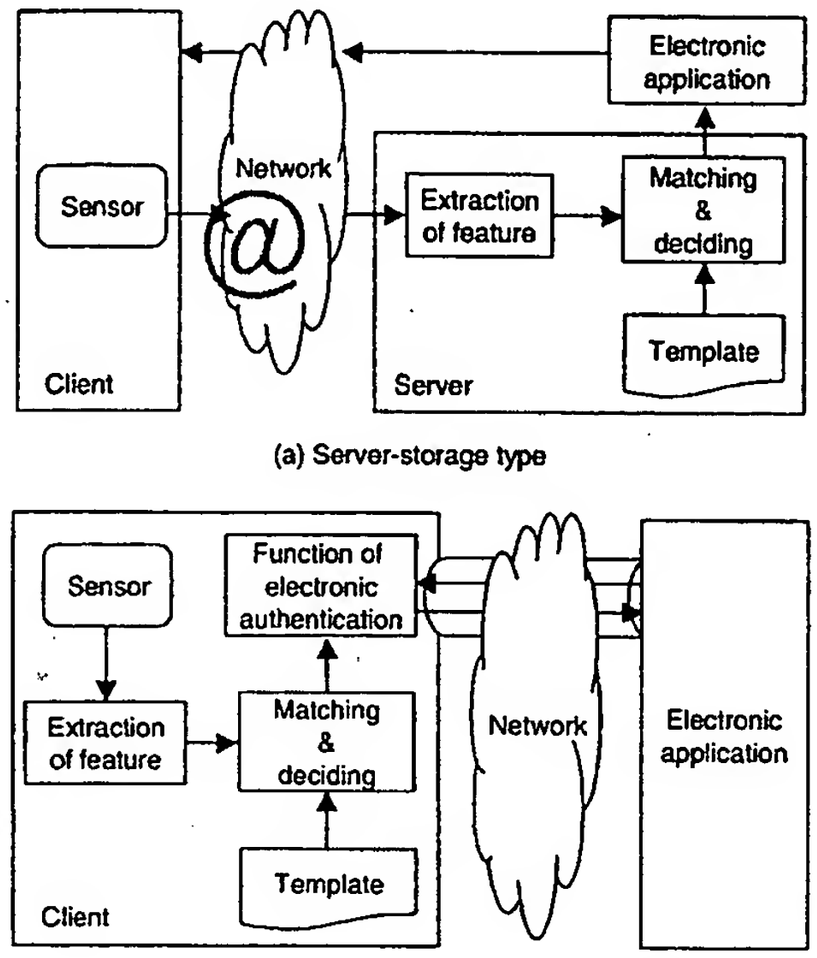
Figure 1. Application of authentication

2.3. Personal authentication over a network

We are studying the following methods of personal

authentication over a network.

- Template storage on the client side (Fig. 1 (b))
- Template storage on the server side[12] (Fig. 2 (a))
- Template storage in portable terminals (Fig. 2 (b))
- Template storage in smart cards (Fig. 2 (b))



(a) Server-storage type

(b) Smart card or portable terminal-storage type

Figure 2. Biometrics authentication on a network

Table 1. Comparison of template storage locations

Storage Place	Advantages	Disadvantages
Server	- The correctness of the template can be judged - All terminals are available - Maintenance costs are low	- Authentication is not possible when the server is downExpensive to build a DB - Heavy DB load - It cannot authenticate the sensor data
Client	- It can authenticate without using a network - An individual can manage a template	- The correctness of the template cannot be judged - Can't Select terminals - Maintenance costs are high
Smart Card (Portable Terminal)	- All terminals are available - Maintenance costs are low individual can manage a template	- The correctness of the template cannot be judged

When the template resides in the server, the user's biometric data that is acquired by sensors on the client side is transmitted to the server, where it is compared with the template that was registered in advance at the server to accomplish personal authentication.

When the template resides in a smart card or portable terminal, the user's biometric data is compared with the template that was registered in advance on the client side and the electronic authentication is performed on the server side to accomplish personal authentication.

Table 1 lists the advantages and disadvantages of storing the template in a smart card or portable terminal and storing it in the server or client.

With the server-template method, templates are managed in the server, so the validity of the template is guaranteed secured by the server's access rights. This method, however, increases the server construction cost because the processing load and risk of attack are concentrated on the server. Also, because the template is private data managed by another party, this method's acceptability to the user is low.

In contrast, storing the template in a smart card (or portable terminal) allows the templates to be managed by the individual, which, in addition to being more acceptable to the user, has the benefit of distributing the security risk. Furthermore, when used in combination with electronic authentication by means of a concealed private key, this method makes it possible to confirm the validity of matching processing that is performed over a network.

The validity of the template with the user ID (in the case of a private key) depends on how resistant the smart card or other such device is to tampering (counterfeiting or corruption). As a measure preventing tampering with registered data in the smart card, confirming the validity of the template by digital signature techniques that use public-key encryption is important.

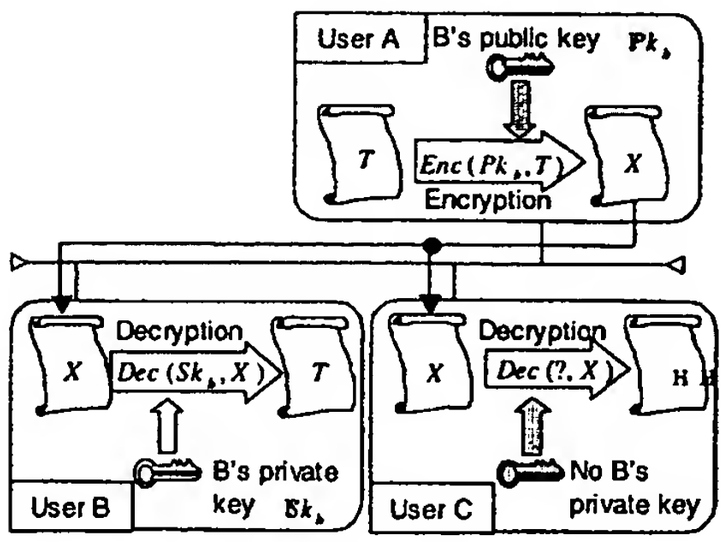
Here, we report on a personal authentication system that deals with the issue of the validity of the template that is registered in the smart card by employing digital signatures as described above.

3. Study of personal authentication system technologies

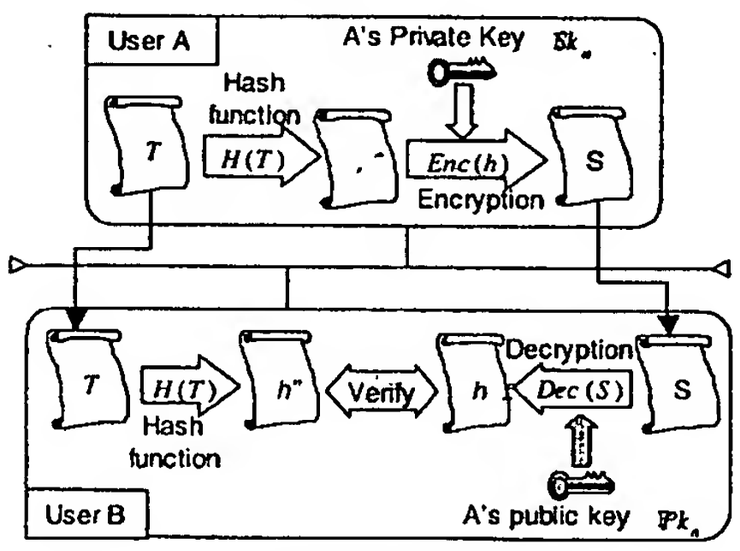
3.1. Overview of public-key encryption technology and X.509 Certificate

3.1.1. Public-key encryption technology[10]

Public-key encryption uses an asymmetrical encryption key pair. An encryption uses one key of the pair, and decryption use the other key of the pair. Each user is issued a pair of keys. One key of the pair is published and is called the public key; the other key is kept secret and is called the private key. Such public-key encryption systems can be used in two ways: for



(a) Kept secret



(b) Digital Signature

Figure 3. Public key encryption system

encryption and for digital signatures (Fig. 3).

When used for encryption, the data to be sent to another party is encrypted by using the public key of the recipient and then transmitted to that party. The receiver then uses their own private key to decrypt the data when it is received. If the secrecy of the private key is maintained, the secrecy of the data is guaranteed.

When used for digital signing, the data that is to be signed is first compressed by using a unidirectional and collision-free conversion function that is called a hash function. The signer then sends the data encrypted with the signer's own private key together with the original data. The receiver uses the sender's public key to decrypt the encrypted data, compresses the original data with the hash function, and checks for consistency in the hash values. This process can validate the owner's public key without corrupting the signed data. The digital signature $Sig(Sk_a, T)$ of the plaintext T using the private key Sk_a is defined by the following equation.

$$Sig(Sk_a, T) = Enc(Sk_a, H(T))$$

Here, the expression $Enc(K, \bullet)$ represents the encryption processing with the key K, and $H(\bullet)$ represents the processing of the hash function. The signature can be validated by evaluation of the following equation.

$$H(T) = Dec(Pk_a, Sig(Sk_a))$$

Here, the expression $Dec(K, \bullet)$ represents the decryption processing with the key K.

3.1.2. X.509 certificate

Building of the social platform to guarantee the integrity of the public key is necessary so that we may apply public-key cipher technology in the open network. The standardized X.509 certificate is the ISO/IEC/ITU standard form of the digital signature used to guarantee the integrity of this public key. Figure 4 shows the construction of the X.509 certificate.

An X.509 certificate was standardized as an authentication function in the X.500 directory service. An X.500 directory service is a standard about the guidance and the offer to the resource in networks. Because the access information of the issuing organization of the certificate is contained in the certificate, the availability of the integrity confirmation management of the certificate is held itself. And, when a public-key base is employed, the X.509 certificate is expanded about the demanded information. All users can judge how trustworthy the

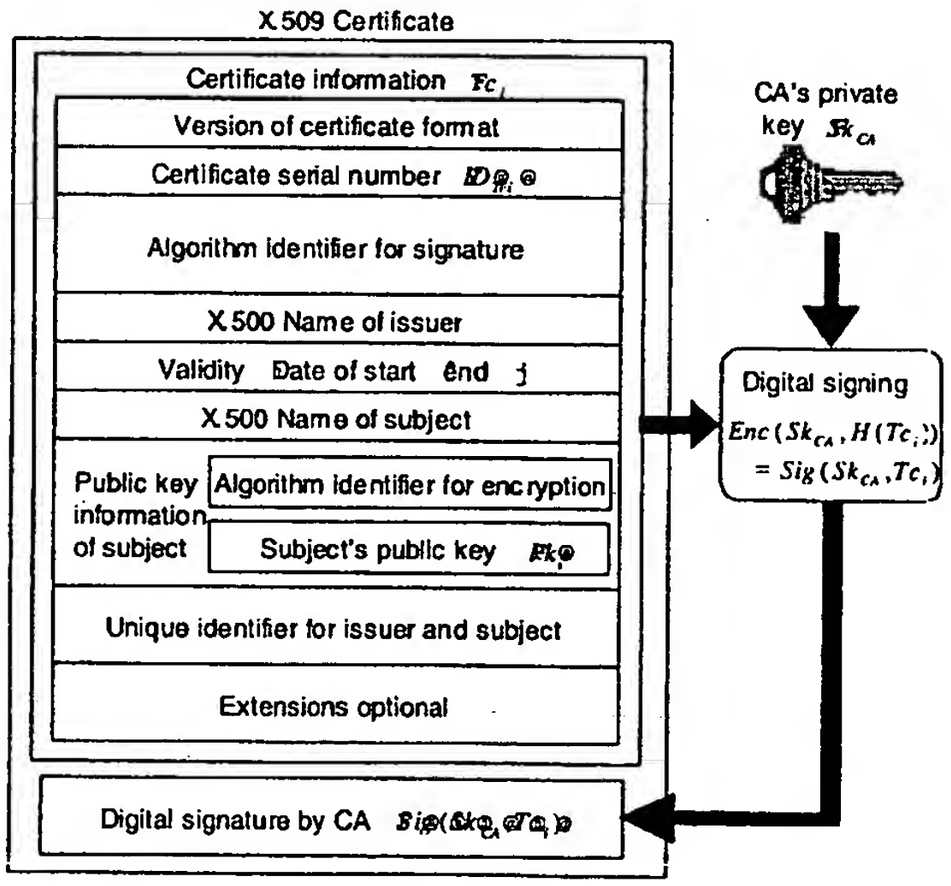


Figure 4. X.509 Certificate[10)]

issuer of the certificate is by referring to the practical use policy, the limitation of the certificate pass, the certificate scrapping list, and so on. We built our personal authentication system according to the X.509 certificate, because we assume the system will be used widely in open network environments.

3.2. Proposal personal authentication system with public-key encryption technology

A personal authentication that employs a combination of public-key encryption technology and biometric personal authentication technology is shown in Fig. 5.

We give the following the flow that application in the system. Our proposal is a user i through a network as to the person authentication.

(1) Process of verifying the integrity of the template:

(i) The template is kept on the terminal that it is signed by the application's private key Sk_A with an administrator of the application confirms the data integrity.

(ii) The application's public key Pk_A is used to verify the integrity of the template for use in the matching process.

(2) Matching process:

(i) This matches the biometric data of a user i inputted to the terminal and a template TD_i.

(ii) If the biometric data corresponds to the template, the terminal is unlocked so that it can use the user's private key Sk_i, which carries out the electronic authentication as a result of the matching.

(3) Electronic authentication process:

(i) The application sends random numbers Rd to the terminal.

(ii) The terminal signs by user i's private key Sk_i, and send back a digital signature $Sig(Sk_i, H(Rd))$ in the terminal to the application.

(iii) The application verifies the signature by using the user's public key Pk_i and Rd.

In the case of cooperation between public-key encryption technology and biometric personal authentication technology as mentioned above, the following results can be considered.

- Improvements in measures to prevent attack:
  - The validity of personal authentication processing that is executed over a network can be guaranteed.
  - The validity of the identity of the owner of the private key can be confirmed by the use of biometrics data.
- Improvement in ease of use:
  - Users can be authenticated simply and conveniently by biometrics authentication.

When further used in combination with smart card technology, the following results can be considered.

- Improvements in measures to prevent attack:
  - The secrecy of the private key in public-key encryption can be guaranteed.
  - Binding the use of the private key only at the biometrics verification time can be included in the smart card.
- Improvement in ease of use:
  - Electronic authentication can be accomplished without selecting terminals by the smart card with the public key data and the biometric data.

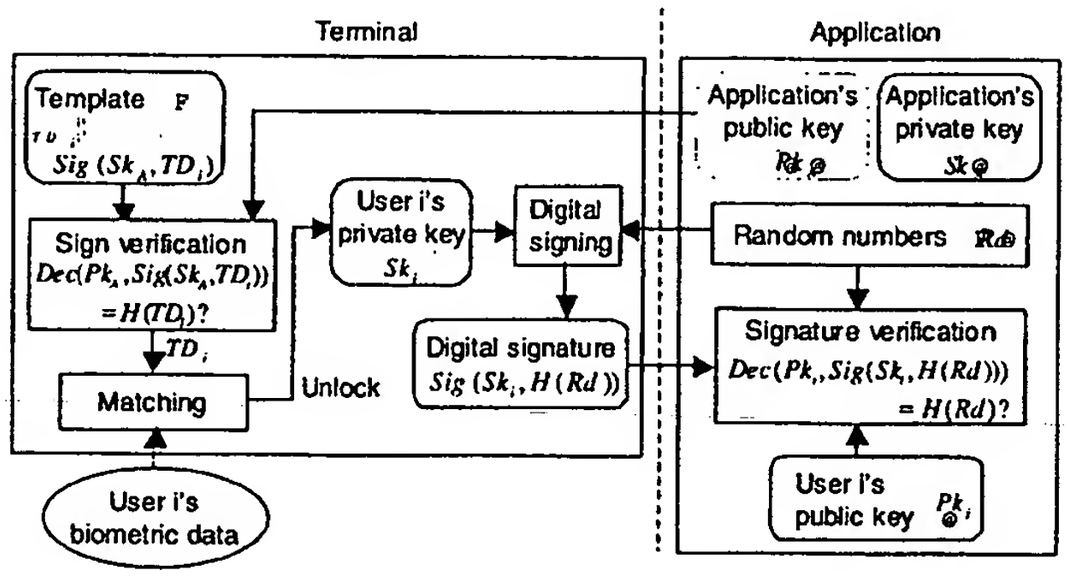


Figure 5. Proposed network authentication system

Table 2. Problems and measures to prevent attack

	Problems	Counter-measures	Effects
PKI	- Collection of private key holder - Secrecy of private key	Biometrics	- Ease of use
	-	Storage in smart card	- Availability - Measures to prevent attack
Smart Card	- Collection of smart card holder - Collection of storage data	Biometrics	- Measures to prevent attack
	-	Digital signature	- Measures to prevent attack
Biometrics	- Collection of Authenticating Process - Privacy	Digital authentication	- Measures to prevent attack
	-	Storage in smart card (Individual management)	- User acceptability - Availability

- Improvement in user acceptability:
  - The template is private data, and can be managed by the individual.

The above advantages are summarized in Table 2.

As shown in Table 2, each of these technologies has its own advantages and disadvantages. By systematically combining biometric personal authentication technology with smart card technology and public-key encryption technology, it is possible to guarantee the validity of personal authentication over an open network.

3.3. Flow of the authentication process in proposed personal authentication system

The following data is stored in the smart card.

- X.509 certificate
- Signed template
- Private key

The correspondence between the template and the X.509 certificate as the user's ID is not guaranteed. Thus, the threat posed by forgery of the certificate or the template or corruption of the smart card as shown in Fig. 6 must be considered.

The template and the ID data must both be digitally signed to ensure correspondence with the X.509 certificate, and thus prevent impersonation through tampering with the smart card. Here, to validate the issuer of the template and maintain the ability to confirm the validity of the template, it is necessary that the template data must confirm to X.509. The template data structure is shown in Fig. 7.

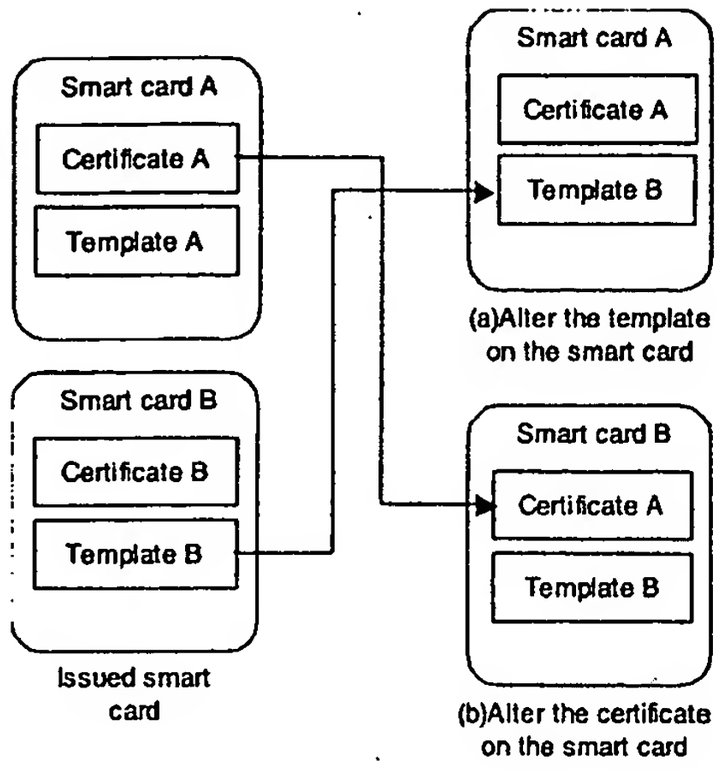


Figure 6. Attack on the smart card

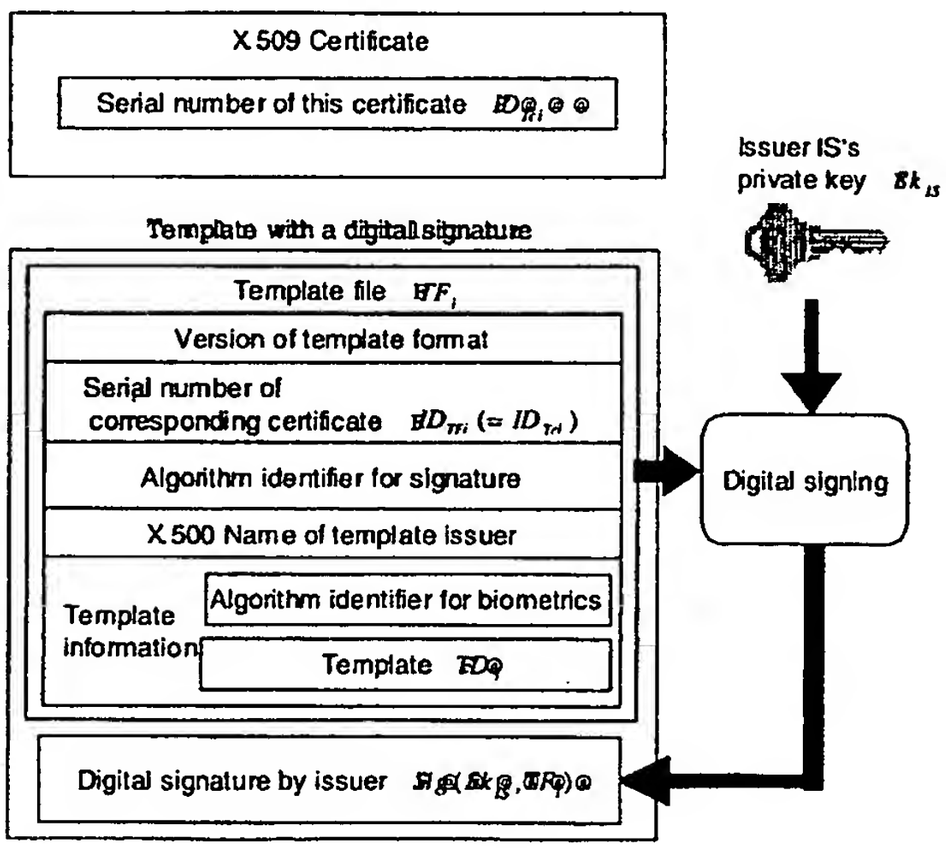


Figure 7. Data structure of template with digital signature

The personal authentication processing procedure in our method for clarifying the correspondence relationship is shown in Fig. 8.

(1) The validity of the X.509 certificate is confirmed by means of the public key of the Certificate Authority Pk_{CA}.

(2) The correspondence relationship is confirmed by means of the X.509 certificate serial number ID_{Tc}

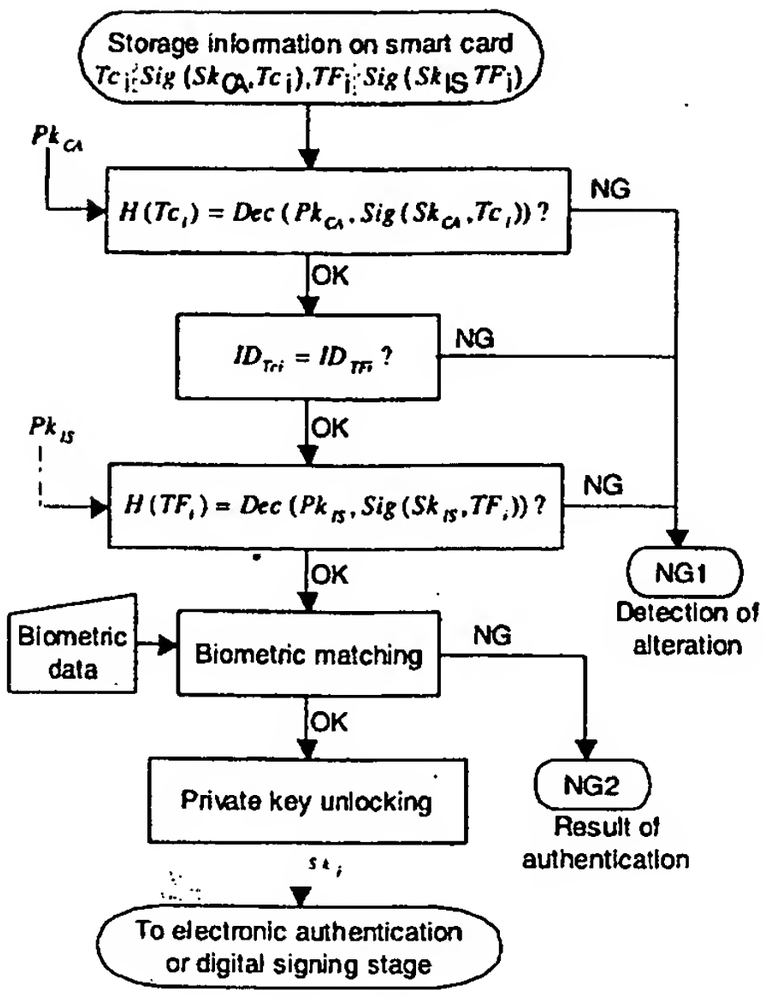


Figure 8. Proposed authentication process

and the template serial number ID_{TF}.

(3) The validity of the template data TF is confirmed by the template issuer's public key Pk_{IS}.

(4) The identity of the smart card's holder is confirmed by matching the template data and the input biometric data.

4. Development of the prototype system

We have developed a prototype system of the above scheme for a groupware application.

The groupware system has biometric personal authentication in an approval of the workflow in the organization. A requirement of any personal authentication system is that it be socially acceptable. In Japan, signatures and fingerprints are accepted as paper-based authorization. In the work reported here, we have developed a prototype that uses fingerprints. We describe the architecture, functions, and results of this prototype system.

4.1. System configuration

The personal authentication infrastructure of the prototype system is shown in Fig. 9.

- Issue processing
  - Registration terminals: Collect personal data containing biometric data.
  - Certificate Authority: Issues X.509 certificates.
  - The issue system: Generates public and private keys (Pk_i, Sk_i) and templates; embeds the data in smart cards and issues them.
- Authentication processing
  - Groupware server: Provides and controls the various functions of the groupware server.
  - Client PC: Performs groupware decision processing by means of personal authentication through the use of fingerprints and smart cards.

To construct this system, we used the groupware software Groupmax Ver. 5*, a product of Hitachi Works. With Groupmax, it is possible to electronically define the work approval flow, such as the circulation of forms and so on, and operate the system in accordance with the tasks of the organization into which the system is introduced.

For the digital signatures and electronic authentication, we used the public key encryption library Keymate/Crypto Ver. 2. 0*.

For the smart cards, we employed the IE-8A(U8)** smart cards and M-650A** read/write device.

4.2. System functions

The developed systems provide the following functions.

(1) Registration terminals (*r*)

- These serve as the clients of the issue system; user data is acquired from multiple terminals.
- User i's personal data and fingerprint image are collected.
- Electronic authentication to confirm the validity of the issue system is performed and the collected data is sent.

(2) Certificate Authority (CA)

- Electronic authentication to confirm the validity of the issue system is performed.
- An X.509 certificate $Tc_i \| Sig(Sk_{CA}, Tc_i)$ is issued for the public key that was generated by the issue system.

(3) Issue system (IS)

- The validity of the biometric data registration terminals and the Certificate Authority are electronically authenticated.
- The collected user i's personal information is provided for the issue operator (preliminary inquiry).

---

* Each products of Hitachi, Ltd.
** Each products of Hitachi Maxell, Ltd.

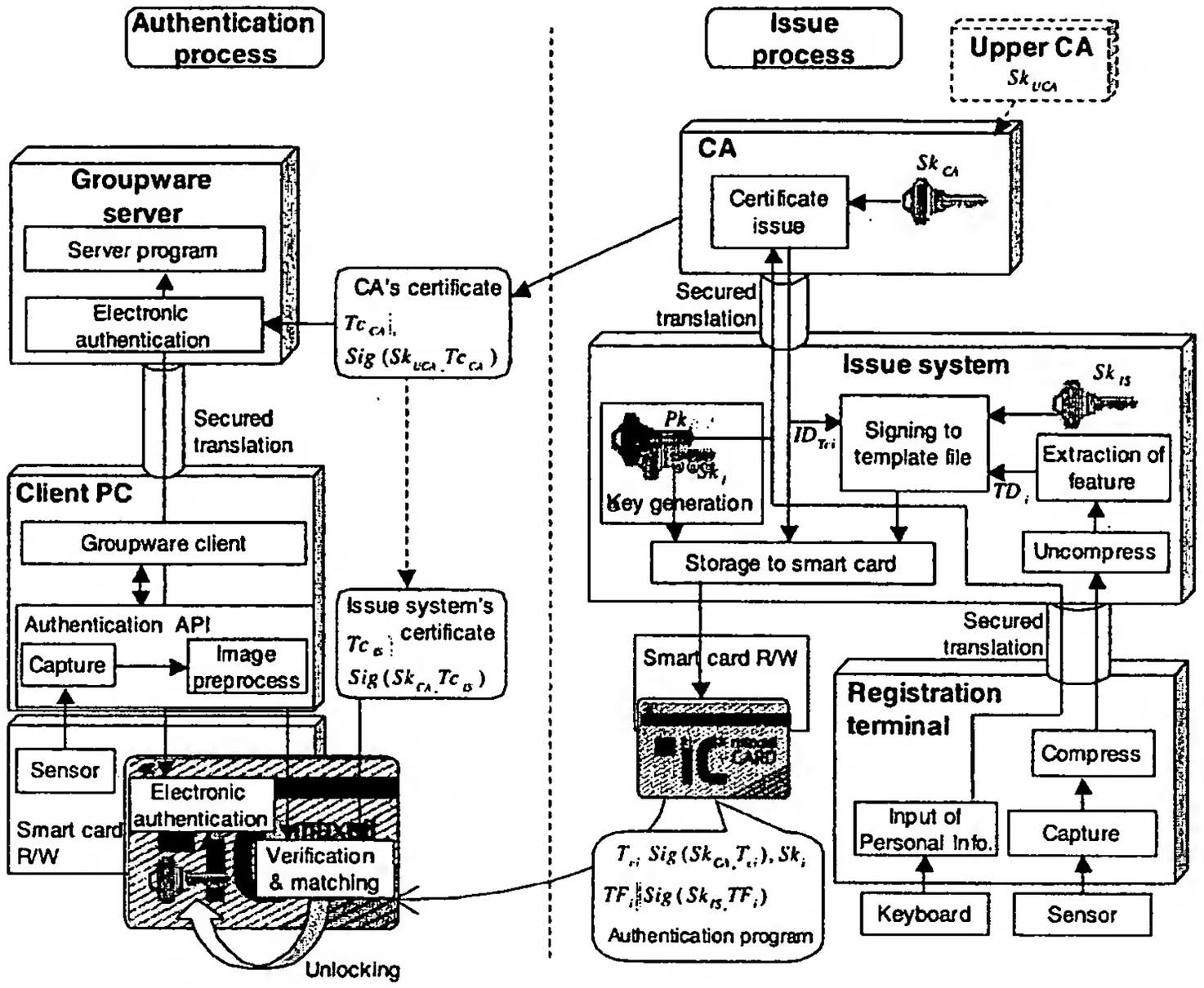


Figure 9. Concept of proposed authentication infrastructure system

- Template TD_i, whose features are extracted from the collected fingerprint images, is generated.
- Public and private keys (Pk_i, Sk_i) are generated for the user i, and entrusted to the Certificate Authority so that an X.509 certificate can be issued.
- The template TD_i and the serial number of the X.509 certificate are signed using the private key (Sk_{IS}) of the issue system.
- User i's private key (Sk_i), the X.509 certificate, and the signed template are written to a smart card, which is then issued as user i's smart card.

(4) Client PC

- The personal authentication process is called from the work approval flow of the groupware client program.
- In the personal authentication process, the validity of the data that is stored in the smart card is confirmed with the digital signature, and the validity of the smart card's holder is confirmed using her or his fingerprint. This process runs between the client PC and the smart card. Fingerprint matching is done in the smart card using pre-image processing by the client PC. The private key is unlocked when the matching process matches the fingerprint data. And it is made response of digital authentication into the smart card. Thus the private key of our proposal system is secured secret in smart card.

(5) Groupware server

- The groupware server can create the groupware work approval flow and forms.
- The groupware server can incorporate the proposed personal authentication function in the approval process by defining it as a plug-in function in the work approval flow electronic form definition.

4.3. Results

Applying the proposed personal authentication system to groupware

- Increases the level of user acceptability:
  - The individual user can manage the private fingerprint data.
- Increases availability:
  - The system does not need a network in the personal authentication processing if a certificate

from the Certificate Authority is obtained in advance.

- Improves ease of use:
  - The system authenticates without the network and thereby improves ease of operation and reduces authentication time.
- Strengthens measures against threats:
  - It is impossible for an unauthorized person to alter the template or the digital signature.
  - It is impossible for an unauthorized person to alter the matching process.
- Increases social acceptability:
  - Electronic authentication of decisions by fingerprint is possible. (Thumbprints are widely used as paper-based authentication in Japan)

5. Conclusion

We have described a biometrics-based personal authentication system in which smart card technology, X.509 certificate technology, and fingerprint verification technology are combined to guarantee the validity of the template. We have also developed a prototype system in which this authentication system and a X.509 digital signature are used in a groupware application. The results confirm that availability is increased and that measures taken to prevent impersonation are strengthened.

The legal aspects of using the personal authentication system described in this report are currently being considered for application to construction on a public key platform such as the digital signature method[11] by means of the same X.509 platform. When biometric personal authentication is applied to such a wide range of users, one problem will be those individuals for whom the fingerprint is objectionable as a means of personal authentication. To address this problem, we have designed our authentication system so that it is not limited to the fingerprint method; rather, the type of biometrics data that is best suited to the user can be selected and registered, or else many types of biometrics data can be registered at the same time if the user so requires. Future work will investigate a system for these applications.

Acknowledgements

We thank Masaji Aoki of Hitachi, Ltd. Information Systems Business Office and Morimi Kuroda of Hitachi Engineering Co., Ltd. for their stimulating discussions over the course of this work.

This work was, in part, conducted under the "Research and Development of a Common Multimedia Platform" research commissioned by the Telecommunications Advancement Organization (TAO) of Japan in 1998.

References

[1] Special Issue on Automated Biometric Systems, Proc. of the IEEE, Vol. 85, No. 9 (1997).

[2] A. Jain et al., eds.: BIOMETRICS Personal Identification in Networked Society, Kluwer Academic Publishers (1999).

[3] ECOM (The Electronic Commerce Promotion Council of Japan) Personal Authentication Technology Study WG: Standards for Evaluation of Personal Authentication (First Ed.), ECOM Report, H9-WG06, http: //www. ecom. or. jp/about wg/wg06/h9doc/wg06-list.htm (1998).

[4] G. Lisimaque: Biometrics and Smart Cards, The Biometric Consortium Fall '99 Conference, Proc. (1999).

[5] Y. Seto: Personal Authentication through the use of Biometrics, The Society of Instrument and Control Engineers of Japan (SICE), Vol. 37, No. 6, pp. 395-401 (1998).

[6] M. Mimura et al.: Development of a personal authentication system using a smart card and fingerprints, Proceedings of Computer Security Symposium '98 (CSS'98), Information Processing Society of Japan (IPSJ) Symposium Series, Vol. 98, No. 12, pp. 185-188 (1998).

[7] Y. Isobe et al.: A Proposal for Authentication System using a Smart card with Fingerprints, Information Processing Society of Japan SIG Notes 99-CSEC-4 Vol. 99, No. 24, pp. 55-60 (1999).

[8] Special Issue: Biometric Personal Authentication Systems up to Now, Journal of the Information Processing Society of Japan, Vol. 40, No. 11 (1999).

[9] EMV'96 Integrated Circuit Card Specification for Payment Systems, ver.3.1.1, http://www.emvco.com/ (1998).

[10] W. Ford, et al: Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Prentice Hall (1997).

[11] "Electronic Authentication," Introduced April 2001, Nikkei Shinbun, Aug. 4, 1999.

[12] M. Negin, et al: An Iris Biometric System for Public and Personal Use, IEEE Magazines: Computer Magazine, Vol. 33, No. 2,pp. 70-75 (2000).